

Secret key rates for an encoded quantum repeater

Sylvia Bratzik,* Hermann Kampermann, and Dagmar Bruß

Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, 40225 Düsseldorf, Germany.

(Dated: January 28, 2014)

We investigate secret key rates for the quantum repeater using encoding [L. Jiang *et al.*, Phys. Rev. A **79**, 032325 (2009)] and compare them to the standard repeater scheme by Briegel, Dür, Cirac, and Zoller. The former scheme has the advantage of a minimal consumption of classical communication. We analyze the trade-off in the secret key rate between the communication time and the required resources. For this purpose, we introduce an error model for the repeater using encoding which allows for input Bell states with a fidelity smaller than one, in contrast to the model given in [L. Jiang *et al.*, Phys. Rev. A **79**, 032325 (2009)]. We show that one can correct additional errors in the encoded connection procedure of this repeater and develop a suitable decoding algorithm. Furthermore, we derive the rate of producing entangled pairs for the quantum repeater using encoding and give the minimal parameters (gate quality and initial fidelity) for establishing a nonzero secret key. We find that the generic quantum repeater is optimal regarding the secret key rate per memory per second and show that the encoded quantum repeater using the simple three-qubit repetition code can even have an advantage with respect to the resources compared to other recent quantum repeater schemes with encoding.

PACS numbers: 03.67.Hk, 03.67.Dd, 03.67.Bg

I. INTRODUCTION AND MOTIVATION

Quantum repeaters [1, 2] are a necessary tool for long-distance quantum communication. They permit to establish entangled Bell pairs over distances of several hundreds of kilometers. A quantum repeater setup consists of segments of small distances, where entangled Bell pairs are created and then entanglement swapping [3] with the neighboring pairs is performed. In order to overcome the decrease in the fidelity due to swapping, entanglement distillation [4, 5] can be performed. There are several suggestions for experimental realizations of quantum repeaters [6, 7]. For a recent review on quantum repeaters, see [8].

Recently, we investigated the optimal quantum repeater setups with respect to the secret key rate [9, 10]. The limiting factor of these quantum repeater schemes, especially regarding the repeater rate, can be the classical communication time to acknowledge the success of entanglement distillation [11]. To overcome this bottleneck, the quantum repeater using quantum error-correcting codes [11, 12] was developed. In these protocols, classical communication is only needed between the neighboring repeater stations.

In this paper we investigate the difference in the secret key rates between the quantum repeater using distillation (*generic quantum repeater*) and the quantum repeater using quantum error correcting codes (*encoded quantum repeater*) by employing the analysis developed in [10] for the generic quantum repeater. As a representative for the encoded quantum repeater we choose [11]. We analyze the trade-off between the communication time and the needed resources. For this purpose, we modify the analysis given in [11] by using a concatenated error model for which we obtain a bound for the fidelity. Our model does not need a fault-tolerant preparation of the initial states, as it handles input pairs which are depolarized states with fidelity $F_0 < 1$. This approach saves

resources, compared to [11], where multi-qubit errors are either suppressed or avoided via distillation. Furthermore, we show how to correct additional errors in the encoded connection procedure and we develop a decoding algorithm suitable for quantum key distribution. We derive the rate for generating entangled pairs with the encoded quantum repeater and use it to calculate secret key rates.

The paper is organized as follows: in Sec. II we first briefly review the repeater scheme from Ref. [11]. Furthermore, the error model and its effect on the quantum states is introduced. We show which errors can be corrected during the encoded connection step and develop an appropriate decoding procedure. We then derive the repeater rate for the encoded quantum repeater scheme, i.e., the average number of entangled Bell pairs per second. In Sec. III, we review the generic quantum repeater, which uses distillation instead of quantum error-correcting codes. Then we provide the threshold parameters for the encoded quantum repeater for obtaining a nonzero secret key rate. We continue to calculate the optimal secret key rate of these quantum repeater protocols and point out where our analysis differs from the original proposal of the encoded quantum repeater scheme [11]. We then present a short analysis of the cost function which was introduced recently in [13]. We conclude in Sec. IV.

II. ENCODED QUANTUM REPEATER SCHEME AND SECRET KEY RATES

In this section we introduce for the quantum repeater using encoding [11] (in the following called *encoded quantum repeater*) a generic error model, show its effect in the different steps of this quantum repeater model and derive the repeater rate, which is needed to calculate the secret key rate.

* bratzik@thphy.uni-duesseldorf.de

A. Principles of the encoded QR

The principle of the encoded quantum repeater is depicted in Fig. 1: the first step is to distribute Bell pairs between the neighboring repeater stations, it follows the encoding operations [step 1) in Fig. 1] and an entanglement swapping scheme [step 2)] which allows to obtain error information. The error information reveals the necessary rotation in order to get a specific encoded Bell pair in the end [step 3)]. The details for entanglement swapping and classical error correction are described in [11]. The encoded quantum repeater was developed for any CSS-code [14, 15].

For simplicity, we will consider the three-qubit repetition code throughout this paper¹. In the ideal case the encoded state ρ_{enc} , shared between the repeater stations R_i and R_{i+1} at step 1) is of the form $\rho_{\text{enc}} = |\tilde{\phi}^+\rangle\langle\tilde{\phi}^+|$ with

$$|\tilde{\phi}^+\rangle = \frac{1}{\sqrt{2}} |000\rangle_{R_i} |000\rangle_{R_{i+1}} + |111\rangle_{R_i} |111\rangle_{R_{i+1}}. \quad (1)$$

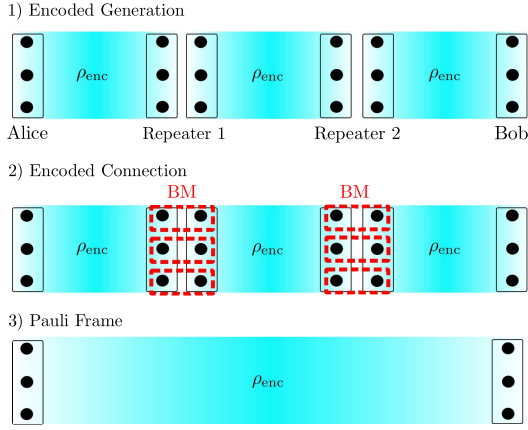


FIG. 1. (Color online) Setup of the encoded quantum repeater (adapted from [11]), BM stands for Bell measurement. In the ideal case $\rho_{\text{enc}} = |\tilde{\phi}^+\rangle\langle\tilde{\phi}^+|$ with $|\tilde{\phi}^+\rangle$ defined in Eq. (1).

1. Error models

Analogously to [2, 11], we will employ the depolarizing error model for all two-qubit gates, thus the unitary operation $U_{i,j}$ acting on qubits i and j is replaced according to the following map $\Lambda(\rho)$:

$$U_{i,j}\rho U_{i,j}^\dagger \rightarrow (1-\beta)U_{i,j}\rho U_{i,j}^\dagger + \frac{\beta}{4}\text{tr}_{i,j}(\rho) \otimes \mathbb{1}_{i,j} =: \Lambda(\rho), \quad (2)$$

¹ We will see in Sec. III D that this simple code leads to a good ratio of the secret key rate and the required resources.

where β is the gate error parameter. We further assume no misalignment and errorfree one-qubit operations². We define

$$U^a := \mathbb{1}_{\{1,\dots,N\}\setminus\{i_a,j_a\}} \otimes U_{i_a,j_a}, \quad (3)$$

to be the unitary operation acting on the two qubits (i_a, j_a) and the identity on the remaining $N-2$ qubits. The vector $\vec{U} = \{U^1, \dots, U^n\}$ defines the sequence of applications of the unitary operations: first one applies the gate U^1 on the qubits i_1, j_1 , then U^2 and so on. For our analytical analysis we will approximate the concatenation of n two-qubit gates by assuming that not more than one gate acts in a faulty way (which corresponds to an expansion in β , keeping only terms in zeroth and first order). Normalization is guaranteed by adding the worst case density matrix (i.e., the identity) for the remaining probability.

Thus, the resulting map $\Lambda_{\text{conc}}(\rho)$ is:

$$\Lambda_{\text{conc}}(\rho) := (1-\beta)^n \left(\prod_{a=1}^n U^a \right) \rho \left(\prod_{a=1}^n U^a \right)^\dagger + n\beta(1-\beta)^{n-1}\tilde{\rho} + p \frac{\mathbb{1}_d}{d}, \quad (4)$$

where $d = \dim(\rho)$, $\mathbb{1}_d$ is the $d \times d$ -identity matrix, and $p = 1 - (1-\beta)^n - n\beta(1-\beta)^{n-1}$. For small β we can expand p in $p \approx \frac{n(n-1)}{2}\beta^2 - n\binom{n-1}{2}\beta^3$, thus p is in the order of β^2 for an appropriate n . The normalized state $\tilde{\rho}$ is given by the map $\Lambda_{1\text{-faulty}}(\rho)$

$$\tilde{\rho} = \frac{1}{n} \sum_{a=1}^n \left(\prod_{b=a+1}^n U^b \right) f\left[(i_a, j_a), \rho, \prod_{c=1}^{a-1} U^c\right] \left(\prod_{b=a+1}^n U^b \right)^\dagger =: \Lambda_{1\text{-faulty}}(\rho), \quad (5)$$

with $f[(i, j), \rho, A] := \text{tr}_{i,j}(A\rho A^\dagger) \otimes \frac{\mathbb{1}_{i,j}}{4}$. Thus, $\tilde{\rho}$ represents the convex combination of states where one gate is replaced by the identity matrix in the corresponding subspace. Instead of the first-order approximation map in Eq. (4) one could use the simpler map

$$\tilde{\Lambda}(\rho) := (1-\beta)^n \left(\prod_{a=1}^n U^a \right) \rho \left(\prod_{a=1}^n U^a \right)^\dagger + [1 - (1-\beta)^n] \frac{\mathbb{1}_d}{d}. \quad (6)$$

But our analysis shows a distinct improvement in the secret key rate using the map in Eq. (4).

2. Encoded state generation

The first step performed in the encoded quantum repeater is to generate the encoded Bell state of Eq. (1) between all

² This assumption about errorfree single-qubit rotations can be made as these rotations can be implemented in the classical postprocessing (application of bit-flips on the measurement data).

repeater stations. Thus, the encoded Bell state is denoted as (we drop the indices R_i and R_{i+1} for better readability)

$$|\tilde{\phi}^+\rangle = \frac{1}{\sqrt{2}} |000000\rangle + |111111\rangle. \quad (7)$$

To generate this state one starts with the state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ at one repeater station and with $|000\rangle$ at the other and applies a *teleportation-based controlled-NOT* (cNOT) [16–18]:

$$\begin{aligned} & \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \otimes |000\rangle \\ & \xrightarrow{\text{cNOT}} \frac{1}{\sqrt{2}} |000000\rangle + |111111\rangle. \end{aligned} \quad (8)$$

The teleportation-based cNOT consists of multiple gates and requires Bell pairs as a resources, as shown in Fig. 2. The setup

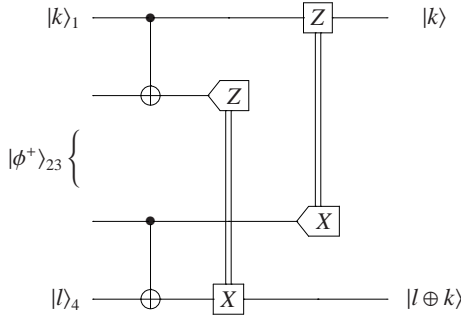


FIG. 2. Teleportation-based cNOT, see [18].

in the encoded quantum repeater is shown in Fig. 3. Between the repeater stations we have a source (S) of Bell states. The teleportation-based cNOT is marked by the red dashed box, i.e., qubits 1 and 2 in Fig. 2 correspond to one black and one yellow (light grey) qubit of repeater station i and qubits 3 and 4 to the qubits of repeater station $i+1$. In total we have three teleportation based cNOTs (see Fig. 3). The total circuit in Fig. 3 consists of 6 two-qubit gates, thus we apply the concatenation of gates as described in the map of Eq. (4). The distributed Bell states are depolarized due to imperfections in the source resulting in ρ_{dep} with fidelity F_0 :

$$\rho_{\text{dep}} = F_0 |\phi^+\rangle \langle \phi^+| + \frac{1-F_0}{3} (\mathbb{1}_4 - |\phi^+\rangle \langle \phi^+|). \quad (9)$$

Different to the proposal in [11], we assume that the initial states do not have fidelity F_0 almost one. Due to the depolarizing error of the quantum operations, see Eq. (2), the state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ (repeater station i in Fig. 3) transforms to³

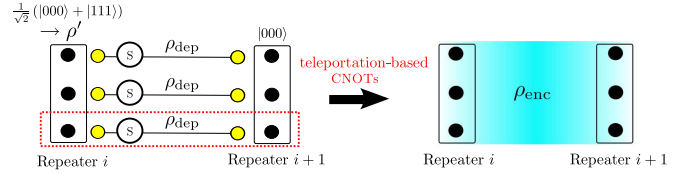


FIG. 3. (Color online) Generation of the encoded state ρ_{enc} (see text).

$$\begin{aligned} \rho' = & \frac{1}{2} \left[1 + \beta \left(\frac{\beta}{2} - \frac{5}{4} \right) \right] (\Pi_{|000\rangle} + \Pi_{|111\rangle}) \\ & + \frac{1}{2} (1 - \beta)^2 (|000\rangle \langle 111| + |111\rangle \langle 000|) \\ & + \frac{\beta}{4} \left(\frac{3}{2} - \beta \right) (\Pi_{|101\rangle} + \Pi_{|010\rangle}) \\ & + \frac{\beta}{8} (\Pi_{|001\rangle} + \Pi_{|110\rangle} + \Pi_{|100\rangle} + \Pi_{|011\rangle}), \end{aligned} \quad (10)$$

where $\Pi_{|klm\rangle} = |klm\rangle \langle klm|$. The state ρ_{enc} after all operations is lengthy and will not be given explicitly here.

3. Encoded connection

In the second step we perform three pairwise Bell measurements (BM in Fig. 1 and Fig. 4) in the repeater station in order to connect two encoded Bell pairs. The results of the

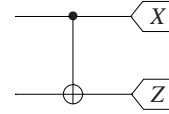


FIG. 4. Circuit for a Bell measurement.

Bell measurements determine the encoded Bell state (see [11] for further explanation). As the three-qubit repetition code is used, we can correct up to one bit-flip error in the measurement results. The bit-flip error is corrected via *majority voting*. Note that the error is corrected classically in the measurement results; no quantum operation is performed on the state.

We denote the map for the total encoded connection $C : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H}')$, where $\mathcal{B}(\mathcal{H})$ is the space of bounded operators with $\dim \mathcal{H} = 2^{12}$ and $\dim \mathcal{H}' = 2^6$. The map consists of the following procedures: Bell measurement, correction of the measurement results and application of the corresponding Pauli matrices in order to obtain $|\tilde{\phi}^+\rangle$ in the end. Note that the action of the Pauli matrices can be replaced by applying bit-flips on the measurement data of the final state. In the following we determine all states $|\varphi_i\rangle \in \mathcal{H}$, such that an application of perfect gates would lead to the correct state, i.e.,

$$C^{\text{perf}}(|\varphi_i\rangle \langle \varphi_i|) = |\tilde{\phi}^+\rangle \langle \tilde{\phi}^+|. \quad (11)$$

³ We obtain this state by applying two faulty cNOTs ($\text{cNOT}_{1 \rightarrow 3}$ and $\text{cNOT}_{1 \rightarrow 2}$) on the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle$.

a. Correctable errors for ideal CNOT The three-qubit repetition code can correct single bit-flip errors. However, due to the properties of the Bell measurement given in Fig. 4 one can correct more errors, which were not considered in the analysis in [11].

If an X error on the control and the target qubit occurs before a perfect $CNOT$ gate, the resulting error after the application of the $CNOT$ is an X -error on the control qubit (see, e.g., [19]). As the Bell measurement is performed by applying a measurement in the X -basis (Z -basis) on the control (target) qubit, this error does not corrupt the measurement result. The same holds also for Y - and Z -errors if they appear both in the control and target qubit of one $CNOT$ (see Fig. 5).

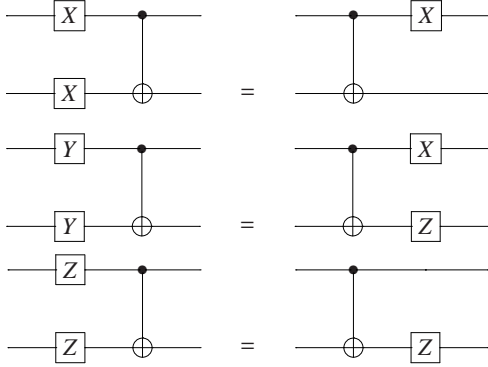


FIG. 5. Commutation rules for the $CNOT$ gates, see [19].

Our analysis shows that considering the correlated X -, Y -, and Z -errors leads to a substantially higher error tolerance for obtaining a nonzero secret key rate. As the error in the gates is only important for the secret fraction in Eq. (27), the secret fraction for different initial fidelities as a function of the gate error parameter β is displayed in Fig. 6. We find that including the correlated error makes the secret key rate more noise-tolerant, where the amount of improvement depends on the initial fidelity F_0 .

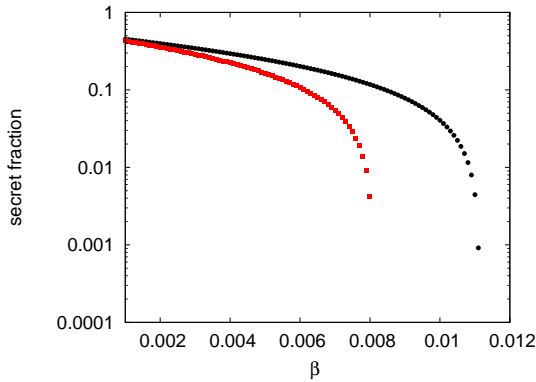


FIG. 6. The secret fraction [Eq. (27)] plotted as a function of the gate error β including all errors according to Eq. (12) (black circles) and those where only single bit-flip errors were correctable (red squares), $F_0 = 0.98$, one repeater station ($r = 1$).

We denote the control (target) qubits of the i -th $CNOT$ gate as c_i (t_i), thus we can correct errors from the set

$$E = \{X_{c_i}X_{t_i}, Y_{c_i}Y_{t_i}, Z_{c_i}Z_{t_i}, \mathbb{1}_{c_i}\mathbb{1}_{t_i}, \mathbb{1}_{c_i}X_{t_i}, X_{c_i}\mathbb{1}_{t_i}\}. \quad (12)$$

Each of the six pairs from the set of errors can happen at one of the three $CNOT$ gates, thus we have $6^3 = 216$ combinations. But some of these combinations have to be excluded, e.g., cases like $\mathbb{1}_{c_1}X_{t_1}\mathbb{1}_{c_2}X_{t_2}\mathbb{1}_{c_3}\mathbb{1}_{t_3}$ are not allowed, as they would lead to a wrong measurement outcome for the majority voting (two X -errors cannot be corrected by the three-qubit repetition code). Excluding these cases 160 combinations remain. We count the number of permutations for three $CNOT$ gates: Fixing, e.g., the combination $X_{c_i}X_{t_i}Y_{c_j}Y_{t_j}Z_{c_k}Z_{t_k}$ with $i \neq j \neq k \in \{1, 2, 3\}$ one has 6 possible permutations of $\{1, 2, 3\}$. In total we have $160 \times 6 = 960$ possible combinations of correctable errors. Let us denote these correctable error as E^i , with $i = 1, \dots, 960$, and the set that contains them as E_{corr} .

The probability of successful entanglement swappings is defined by the overlap of the states to be swapped (ρ_{enc} , see Fig. 1) with the correctable states $|\varphi_i\rangle$. These states $|\varphi_i\rangle$ are computed by the action of correctable errors E^i from the set E_{corr} onto the states $|\tilde{\phi}^+\rangle \otimes |\tilde{\phi}^+\rangle$:

$$|\varphi_i\rangle := E^i(|\tilde{\phi}^+\rangle \otimes |\tilde{\phi}^+\rangle), \quad i = 1, \dots, 960. \quad (13)$$

Out of the 960 correctable states we have 64 distinct orthogonal states, denoted as $|\tilde{\varphi}_i\rangle$. The probability of successful entanglement swapping is thus:

$$p_s = \sum_{i=1}^{64} \langle \tilde{\varphi}_i | \rho_{\text{enc}} \otimes \rho_{\text{enc}} | \tilde{\varphi}_i \rangle, \quad (14)$$

where ρ_{enc} is the output state after the teleportation-based $CNOT$. This probability holds for one repeater station. For r repeaters we can bound the success probability by⁴

$$P_r = (p_s)^r, \quad (15)$$

because we assumed that the errors can be corrected independently. The final state after entanglement swapping is given by:

$$\rho_{\text{swap}}^{\text{ideal}}(r) = P_r |\tilde{\phi}^+\rangle \langle \tilde{\phi}^+| + \frac{(1 - P_r)}{2^6 - 1} (\mathbb{1}_{2^6} - |\tilde{\phi}^+\rangle \langle \tilde{\phi}^+|), \quad (16)$$

i.e.,

$$C^{\text{perf}}(\rho_{\text{enc}} \otimes \rho_{\text{enc}}) = \rho_{\text{swap}}^{\text{ideal}}(r). \quad (17)$$

The state given in Eq. (16) is an estimate; with probability P_r we obtain the perfect state and with probability $1 - P_r$ we obtain the completely mixed state without the perfect state.

⁴ Note that this estimate is a lower bound, as with more entanglement swappings we could certainly correct more errors.

b. Nonideal cNOT The nonideal cNOT operation in the Bell measurements is obtained by using the noise model of Eq. (4):

$$\Lambda_{\text{cNOT}}(\rho) = (1 - \beta)^3 U \rho U^\dagger + 3\beta(1 - \beta)^2 \tilde{\rho} + \left[1 - (1 - \beta)^3 - 3\beta(1 - \beta)^2\right] \frac{\mathbb{1}_{2^6}}{2^6}, \quad (18)$$

where U is the concatenation of ideal cNOTs. The state $\tilde{\rho}$, see Eq. (5), is the convex combination of states where one of the three cNOT gates is replaced by the identity matrix in the corresponding subspace [see Eq. (2)]. The map for encoded connection with imperfect cNOTs acting on the correctable states $|\tilde{\varphi}_i\rangle$ with $i = 1, \dots, 64$ is

$$\begin{aligned} C^{\text{imperf}}(|\varphi_i\rangle\langle\varphi_i|) &= (1 - \beta)^3 |\tilde{\varphi}^+\rangle\langle\tilde{\varphi}^+| \\ &+ 3\beta(1 - \beta)^2 \frac{1}{2} (\Pi_{|000000\rangle} + \Pi_{|111111\rangle}) \\ &+ \left[1 - (1 - \beta)^3 - 3\beta(1 - \beta)^2\right] \frac{\mathbb{1}_{2^6}}{2^6} \\ &=: \rho_s. \end{aligned} \quad (19)$$

The resulting state for imperfect cNOTs after one round of entanglement swapping is given by:

$$\begin{aligned} C^{\text{imperf}}(\rho_{\text{enc}} \otimes \rho_{\text{enc}}) \\ = P_1 \rho_s + \frac{1 - P_1}{2^6 - 1} (\mathbb{1}_{2^6} - |\tilde{\varphi}^+\rangle\langle\tilde{\varphi}^+|). \end{aligned} \quad (20)$$

For more than one repeater station, we use the approximation

$$\begin{aligned} C^{\text{imperf}}(|\varphi_i\rangle\langle\varphi_i|^{\otimes r}) &= (1 - \beta)^{3r} |\tilde{\varphi}^+\rangle\langle\tilde{\varphi}^+| \\ &+ 3^r \beta^r (1 - \beta)^{2r} \frac{1}{2} (\Pi_{|000000\rangle} + \Pi_{|111111\rangle}) \\ &+ \left[1 - (1 - \beta)^{3r} - 3^r \beta^r (1 - \beta)^{2r}\right] \frac{\mathbb{1}_{2^6}}{2^6} \\ &=: \rho_s(r), \end{aligned} \quad (21)$$

which leads to a lower bound on the secret key rate; higher order terms are represented as identity, more useful states could be present.

Finally, the state with r repeater stations after swapping is given by:

$$\begin{aligned} \rho_{\text{swap}}^{\text{nonideal}}(r) &= P_r \rho_s(r) \\ &+ \frac{1 - P_r}{2^6 - 1} (\mathbb{1}_{2^6} - |\tilde{\varphi}^+\rangle\langle\tilde{\varphi}^+|), \end{aligned} \quad (22)$$

with P_r given in Eq. (15).

4. Decoding and final state

In order to do quantum key distribution, one needs to decode the state $\rho_{\text{swap}}^{\text{nonideal}}(r)$ in Eq. (22).

We assume that the decoding procedure is the reverse process of the encoding procedure (see Fig. 7): Alice and Bob each measure two of their three qubits. As we employ the three-qubit repetition code, one can only correct one bit-flip

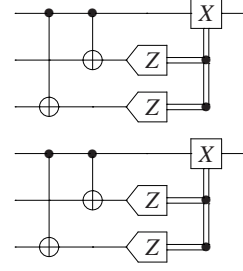


FIG. 7. Decoding procedure: The upper three qubits are on Alice's and the lower are on Bob's side.

error for Alice and Bob. Other errors cannot be corrected by this code. Depending on their measurement results, Alice and Bob have to correct their qubit with a bit-flip operation. If Alice's and Bob's input state was only subjected to one-qubit bit-flip errors, they only have to correct their qubit if their measurement outcome was "11", which is the case when there was a bit-flip error on the first qubit. If an error occurs in the second or the third qubit, the error does not propagate to the first qubit, thus no correction has to be performed.

To obtain the final state which is used for quantum key distribution, we take the state after swapping in Eq. (22) and perform the decoding operation \mathcal{D} :

$$\rho_{\text{dec}} = \mathcal{D}[\rho_{\text{swap}}^{\text{nonideal}}(r)]. \quad (23)$$

The decoding map has the following properties:

$$\mathcal{D}(|\tilde{\varphi}^+\rangle\langle\tilde{\varphi}^+|) = |\phi^+\rangle\langle\phi^+|, \quad (24a)$$

$$\mathcal{D}(\Pi_{|000000\rangle} + \Pi_{|111111\rangle}) = |00\rangle\langle 00| + |11\rangle\langle 11|, \quad (24b)$$

$$\mathcal{D}\left(\frac{\mathbb{1}_{2^6}}{2^6}\right) = \frac{1}{4} |\phi^+\rangle\langle\phi^+| + \frac{3}{4} \left[\frac{1}{3} (\mathbb{1}_{2^2} - |\phi^+\rangle\langle\phi^+|)\right] = \frac{\mathbb{1}_{2^2}}{4} \quad (24c)$$

The first property [Eq. (24a)] follows from the action of the cNOT gates, see Fig. 7:

$$|\tilde{\varphi}^+\rangle \rightarrow |\phi^+\rangle_{1,4}^+ \otimes |0000\rangle_{2,3,5,6}, \quad (25)$$

where the index denotes the number of qubits. The second property [Eq. (24b)] can be shown in an analogous way:

$$\begin{aligned} &\Pi_{|000000\rangle} + \Pi_{|111111\rangle} \\ &\rightarrow (|00\rangle\langle 00|_{1,4} + |11\rangle\langle 11|_{1,4}) \otimes |0000\rangle\langle 0000|_{2,3,5,6}. \end{aligned} \quad (26)$$

The last equality [Eq. (24c)] can be verified by inserting the completely mixed state into the decoding map. Using Eqs. (21) and (22) the state after perfect decoding is given by:

$$\begin{aligned} \rho_{\text{dec}} &= \left[P_r (1 - \beta)^{3r} - \frac{1 - P_r}{2^6 - 1} \right] |\phi^+\rangle\langle\phi^+| \\ &+ P_r 3^r \beta^r (1 - \beta)^{2r} \frac{1}{2} (|00\rangle\langle 00| + |11\rangle\langle 11|) \\ &+ \left[P_r q_r + \frac{(1 - P_r) 2^6}{2^6 - 1} \right] \frac{\mathbb{1}_{2^2}}{4}, \end{aligned} \quad (27)$$

with $q_r = 1 - (1 - \beta)^{3r} - 3^r \beta^r (1 - \beta)^{2r}$.

We can also include gate errors in the decoding, by again using the error model in Eq. (4), leading to the final state:

$$\begin{aligned} \rho_{\text{final}} = & (1 - \beta)^4 \rho_{\text{dec}} \\ & + 4\beta(1 - \beta)^3 \rho_{\text{dec}}^{\text{nonideal}} \\ & + (1 - (1 - \beta)^4 - 4\beta(1 - \beta)^3) \frac{\mathbb{1}_4}{4}, \end{aligned} \quad (28)$$

where $\rho_{\text{dec}}^{\text{nonideal}} = \mathcal{D}_{\text{imperf}}^{\text{nonideal}}(\rho_{\text{swap}}^{\text{nonideal}}(r))$ which is composed of $\Lambda_{1\text{-faulty}}(\rho_{\text{swap}}^{\text{nonideal}}(r))$, see Eq. (5), and applying the correcting operation (see Fig. 7) such that

$$\begin{aligned} \mathcal{D}_{\text{imperf}}^{\text{nonideal}}(|\tilde{\phi}^+\rangle\langle\tilde{\phi}^+|) &= \mathcal{D}_{\text{imperf}}^{\text{nonideal}}\left(\frac{1}{2}(\Pi_{|000000\rangle} + \Pi_{|111111\rangle})\right) \\ &= \frac{1}{2}\left\{\left[\frac{3}{8}(|00\rangle\langle 00| + |11\rangle\langle 11|) + \frac{1}{8}(|01\rangle\langle 01| + |10\rangle\langle 10|)\right] \right. \\ &\quad \left. + \frac{\mathbb{1}_4}{4}\right\} \\ &=: \tilde{\rho}'. \end{aligned} \quad (29)$$

The state $\rho_{\text{dec}}^{\text{nonideal}}$ is given by

$$\begin{aligned} \rho_{\text{dec}}^{\text{nonideal}} = & P_r \left\{ [(1 - \beta)^{3r} + 3^r \beta^r (1 - \beta)^{2r}] \tilde{\rho}' \right. \\ & \left. + \{1 - [(1 - \beta)^{3r} + 3^r \beta^r (1 - \beta)^{2r}]\} \frac{\mathbb{1}_4}{4} \right\} \\ & + \frac{1 - P_r}{2^6 - 1} \left(2^6 \frac{\mathbb{1}_4}{4} - \tilde{\rho}' \right). \end{aligned} \quad (30)$$

We now use the final state ρ_{final} in Eq. (28) to calculate secret key rates.

B. Secret key rate

Analogously to [10], we define the secret key rate per memory per second for the repeater to be

$$K^v = R^v \frac{r_\infty}{M^v}, \quad (31)$$

where R^v is the repeater rate, i.e., the average number of generated entangled Bell pairs per second for the repeater scheme⁵ v , r_∞ is the secret fraction, i.e., the ratio of secret bits and measured bits in the asymptotic limit (Devetak-Winter bound [20]) and M^v is the number of memories used for each protocol. For the three-qubit repetition code employed here, the number of memories per half node of a repeater station is given by

$$M^{\text{QEC}} = 6, \quad (32)$$

as we need six qubits on each side to perform the teleportation-based cNOT (see Fig. 3). The formula for the secret fraction using the six-state protocol [21, 22] can be found, e.g., in Ref. [23]:

$$\begin{aligned} r_\infty = & 1 - e_Z h\left(\frac{1 + (e_X - e_Y)/e_Z}{2}\right) \\ & - (1 - e_Z) h\left(\frac{1 - (e_X + e_Y + e_Z)/2}{1 - e_Z}\right) \\ & - h(e_Z), \end{aligned} \quad (33)$$

where the binary Shannon entropy is given by

$$h(p) = -p \log_2 p - (1 - p) \log_2 (1 - p), \quad (34)$$

and e_X , e_Y and e_Z are the error rates in the X -, Y -, and Z -basis, respectively. The analytic form of the error rates for Bell-diagonal states can be found in [23]. It is possible to perform the analysis in an analogous way for other QKD-protocols such as the BB84-protocol [24].

The remaining term in the secret key rate is the repeater rate R^v , which is the average number of generated entangled Bell pairs per second. For its derivation, we first estimate the average waiting time to distribute the Bell pairs needed for the teleportation-based cNOT (see Fig. 2). The probability of successful generation of one Bell pair over the distance L_0 is

$$P_0 = 10^{-\alpha L_0/10}, \quad (35)$$

with $\alpha = 0.17$ dB/km a realistic photon absorption coefficient for telecom fibers. The probability P_0 corresponds to the transmittivity of photons in an optical fiber with an attenuation length of $L_{\text{att}} = 25.5$ km. In [25] the average waiting time for generating N Bell pairs with probability P_0 is given by

$$\langle T \rangle_N = T_0 Z_N(P_0), \quad (36)$$

where $T_0 = L_0/c$ is the fundamental time (where $c = 2 \times 10^5$ km/s is the speed of light in the fiber) and

$$Z_N(P_0) := \sum_{j=1}^N \binom{N}{j} \frac{(-1)^{j+1}}{1 - (1 - P_0)^j} \quad (37)$$

is the average number of attempts to connect N pairs, see [25]. For the encoded quantum repeater with r repeater stations we need to establish $3(r + 1)$ Bell pairs, thus the repeater rate (the reciprocal value of the average waiting time) for the encoded quantum repeater is given by

$$R^{\text{QEC}} = \frac{1}{\langle T \rangle} = \frac{1}{2T_0 Z_{3(r+1)}(P_0)}, \quad (38)$$

under the assumption that the entanglement swapping process is deterministic, i.e., the probability of successful entanglement swapping is one. The factor 2 in front of the fundamental time T_0 accounts for the time needed to send a photon and acknowledge its arrival. Note that no further classical communication is needed in this repeater protocol. This is contrary to the generic quantum repeater, where after distillation and entanglement swapping in each step the success has to be communicated [10]. We will compare this protocol with respect to the secret key rate to the generic quantum repeater which needs much more classical communication.

⁵ By the repeater scheme v , we mean the scheme mentioned in the introduction: either the encoded quantum repeater ($v = \text{QEC}$) or the generic quantum repeater ($v = \text{QR}$).

III. RESULTS AND COMPARISON OF THE SECRET KEY RATES

In this section, we first investigate the minimally required parameters for obtaining a nonzero secret key for the encoded quantum repeater. Then we find the optimal secret key rate by optimizing over the encoded quantum repeater and the generic quantum repeater model (see [10]).

A. Minimal parameters

Similar to our analysis in [9], we derive for the encoded quantum repeater the minimally required parameters, i.e., the initial fidelity F_0 [for the depolarized state given in Eq. (9)] and the gate quality $p_G = 1 - \beta$ [see Eq. (4)], to obtain a nonzero secret key, see Eq. (31). Table I summarizes the results of our investigations about the minimal fidelities and gate qualities, which are needed to achieve a nonzero secret key rate.

r	N	$p_{G,\min}$	$F_{0,\min}$
1	1	0.984	0.944
3	2	0.993	0.972
7	3	0.994	0.981
15	4	0.996	0.986
31	5	0.997	0.989
63	6	0.997	0.991
127	7	0.998	0.992

TABLE I. Minimal gate quality $p_{G,\min}$ [see Eq. (4) with $p_G = 1 - \beta$ and $F_0 = 1$] and minimal fidelity $F_{0,\min}$ with $p_G = 1$ for extracting a secret key for the six-state protocol, see Eq. (33), with $r = 2^N - 1$ repeater stations, where N is the nesting level for entanglement swapping.

Comparing these numbers to the results for the generic quantum repeater in [9], we find that the encoded quantum repeater is less tolerant against gate errors. This can be expected as many gates are needed for generating the encoded Bell pair. Regarding the initial fidelity F_0 , the encoded quantum repeater also requires fairly good initial Bell states. In Fig. 8, we show the secret key rate for the encoded quantum repeater, optimized with respect to the number of repeater stations, as a function of the gate quality p_G and initial fidelity F_0 , for a fixed distance. We find that a nonzero secret key rate for the encoded quantum repeater is restricted to gate errors below $\beta = 0.0165$ and fidelities above $F_0 = 0.943$.

B. Optimal secret key rates

The purpose of this paper is to investigate whether the optimal secret key rate is reached for the encoded or the generic quantum repeater. By the generic quantum repeater, we mean the repeater scheme using distillation (either the *Deutsch et al.* [5] or the *Dür et al.* [2] distillation protocols, see [10]).

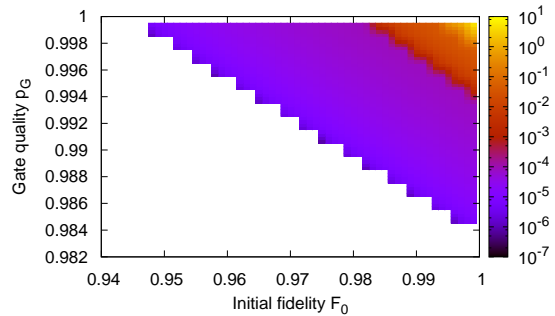


FIG. 8. (Color online) The optimal secret key rate per memory per second, see Eq. (31), as a function of the initial fidelity F_0 and the gate quality p_G , optimized over the number of repeater stations for the encoded quantum repeater ($L = 600$ km). In the white region it is not possible to extract a nonzero secret key.

Figure 9 shows the optimal secret key rate per memory per second [Eq. (31)] for the two different repeater schemes plotted as the function of the distance for some realistic parameters (initial fidelity $F_0 = 0.98$ and gate quality $p_G = 0.992$). We find that the generic quantum repeater leads to an optimal secret key rate that is one order of magnitude better than the encoded quantum repeater. We know from [10] that in this range of parameters it is optimal for the generic quantum repeater to not distill, thus the number of used memories is one in this case. For the encoded quantum repeater, however, we constantly use six memories [see Eq. (32)] which reduces the secret key rate by this factor. In the case of no distillation and deterministic entanglement swapping the encoded quantum repeater is not an advantage for the chosen parameters. Also in regimes where distillation is optimal for the generic quantum repeater (see [10]), we find that the encoded repeater is never better.

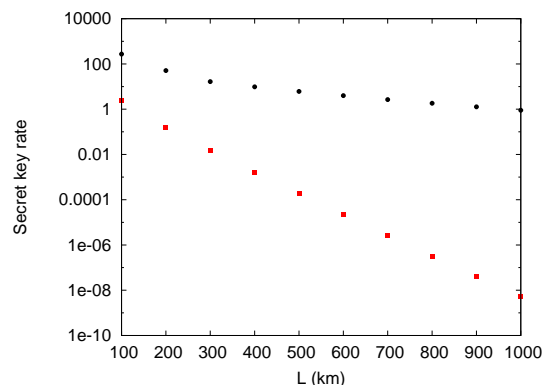


FIG. 9. (Color online) The optimal secret key rate per memory per second in Eq. (31) for the encoded (red squares) and the generic quantum repeater (black circles) as a function of the total distance L (Parameters: $F_0 = 0.98$, $p_G = 0.992$).

C. Comparison to the scheme in Jiang et al.

As mentioned in the introduction, Ref. [11] analyzes the errors of the encoded quantum repeater. Different to their analysis, we allow the initial Bell pairs to have a fidelity $F_0 < 1$, whereas in the original reference fault-tolerant distillation is assumed which would require additional qubits and operations. Also we do not perform fault-tolerant initialization of the codes which has the following advantages: our scheme saves resources and no additional measurements have to be realized. Our error model, see Eq. (4), is a very good estimate, especially for the β resulting from our investigations of the minimal parameters ($\beta = 10^{-2} - 10^{-3}$, see Sec. III A): the probability p for the identity is on the order of 10^{-3} . It means that the distance to a map, where the exact output state is used, is small. We verified this statement for the decoding map (Sec. II A 4) and found that the Uhlmann fidelity of the state in Eq. (28) compared to a state calculated with a map, where all gates with errors are used, is one for the range of β given above. - So far, we do not consider memory and measurement errors, but they could be easily implemented in our analysis.

Another difference in the analysis is the repeater rate. In [11] it was assumed that the generation rate for undistilled Bell pairs with m qubits⁶ available at each station is given by⁷

$$R = m \frac{P_0}{L_0}, \quad (39)$$

using a perfect overall efficiency for collecting and detecting single photons. This is only an appropriate estimate in the case of infinitely many memories. We considered that exactly m Bell pairs to start the encoding process are needed and one has m memories instead of infinitely many memories available. This results in the estimate with the average waiting time as described by Eq. (37) (Sec. II B) and leads to a decrease of the repeater rate [Eq. (38)] by several orders of magnitude⁸ compared to Eq. (39).

D. Cost function

Recently, in [13] a quantum repeater scheme was investigated that only uses one-way classical communication without the necessity to herald the successful generation of entangled Bell pairs between the repeater stations.

In [13], the cost function was defined to be the minimum number of total memory qubits per secret bit:

$$C = \min_{\nu, N} \frac{2^{N+1}}{K^\nu}, \quad (40)$$

where K is the secret key rate as defined in Eq. (31), N is the nesting level and ν is the index for the chosen protocol. The factor 2^{N+1} accounts for the total number of memories (with the number of memories M per half node of the repeater station, see Eq. (32), being implicitly contained in the secret key rate K): $(2^N - 1)2$ is the sum of all memory qubits in the repeater stations ($r = 2^N - 1$). Adding 2 memory qubits from the two communicating parties (Alice and Bob) results in 2^{N+1} memory qubits in total.

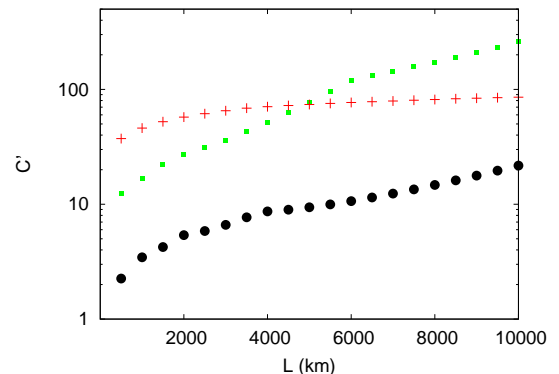


FIG. 10. (Color online) The cost coefficient ($C' = C/L$) [Eq. (40)] for the encoded (green squares), the generic quantum repeater (black circles) and the quantum repeater protocol presented in [13] (red crosses, with the effective qubit error $\varepsilon = 10^{-4}$, for an explanation see [13]) as a function of the total distance L (Parameters: $F_0 = 0.99995$, $p_G = 0.9999$, and $T_0 = 1$ as in [13]).

Figure 10 shows the cost coefficient C' , which is the cost function C [Eq. (40)] divided by the total length L , using the encoded quantum repeater with the three-qubit repetition code, the generic quantum repeater and the repeater protocol presented in [13]. The optimal distillation protocol for the generic quantum repeater is the *Deutsch et al.* protocol. We find that up to 5000 km both the generic quantum repeater and the encoded quantum repeater are below the cost coefficient given in [13]. The generic quantum repeater has a better resource efficiency for all distances. The generic quantum repeater needs less resources and the overhead in classical communication is compensated by fewer numbers of qubit memories used.

In Fig. 11, we show the optimal distance L_0 between the repeater stations for the encoded and the generic quantum repeater as a function of L . We point out that L_0 is in the order of 30 – 120 km, depending on L , while the optimal distance in [13] was given by 1 – 2 km. In the generic quantum repeater scheme the total number of required repeater stations is circa 1 – 2 orders of magnitude smaller than in [13].

IV. CONCLUSIONS

We investigated secret key rates for the so-called *encoded quantum repeater* that utilizes quantum error-correcting codes instead of entanglement distillation as used in the *generic quantum repeater*. The advantage of the former repeater

⁶ Note that $m = M/2$ with M given in Eq. (32).

⁷ The probability of successful transmission P_0 [see Eq. (35)] is equivalent to the expression $\exp(-L_0/L_{\text{att}})$ given in [11].

⁸ The repeater rate and thus the secret key rate can be increased by using multiplexing as shown in [26].

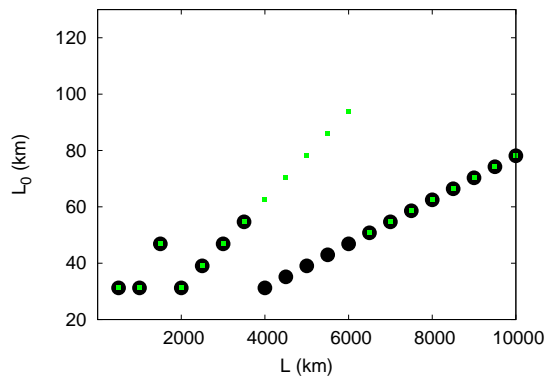


FIG. 11. (Color online) The optimal distance between the repeater stations L_0 for the cost coefficient ($C' = C/L$, see Eq. (40), for the encoded (green squares) and the generic quantum repeater (black circles) (parameters $F_0 = 0.99995$ and $p_G = 0.9999$, $T_0 = 1$ as in [13]) as a function of the total distance L .

scheme is that the classical communication is minimal as it is needed only for the entanglement generation. Before starting to calculate the secret key rate, we improved the error model for the encoded quantum repeater [11] and replaced it by a concatenated one, which leads to a very good estimate of the fidelity. This model permits us to start with Bell pairs with fidelity smaller than one. We also accounted for additional correctable errors for the encoded connection of the encoded Bell states and finally developed a decoding algorithm suitable for the three-qubit repetition code using an analogous error model. We estimated the minimally required parameters for a nonzero secret key and found that for many repeater stations the requirements for the gate quality and the initial fidelity of the Bell pairs are quite demanding. In order to calculate the

secret key rate for the encoded quantum repeater, we derived the rate for generating entangled pairs. The comparison of the secret key rates for the encoded and generic quantum repeater showed that the generic scheme is advantageous for the whole considered range of parameters for the gate quality and the initial fidelity. Finally, we calculated the cost function for the repeater schemes studied here. The cost function determines the required resources divided by the secret key rate. We found that the cost function for the schemes analyzed here is better than the scheme presented in [13], for a wide range of parameters. Furthermore, the number of repeater stations is circa 1 – 2 orders of magnitude smaller than in the latter scheme.

So far, measurement and memory errors are excluded, but can be implemented easily in our analysis. The secret key rate can be improved by applying multiplexing (see, e.g., [26]). As we performed the calculations on density matrices, the quantum error-correcting codes used here for the encoded quantum repeater are limited to a small number of qubits. As an example we treated the three-qubit repetition code. We showed that even with this simple quantum error-correcting code we can have an advantage regarding the cost function over complicated schemes using more resources. We conjecture that utilizing more sophisticated codes (see, e.g., [11]) does not lead to an increase of the secret key rate, as more resources are needed especially when the encoding is performed with errors.

ACKNOWLEDGMENTS

The authors thank Michael Epping, Sreraman Muralidharan, and Liang Jiang for discussions. The authors acknowledge financial support by the German Federal Ministry of Education and Research (BMBF, project QuOREP).

-
- [1] H.-J. Briegel, W. Dür, J. Cirac, and P. Zoller, *Physical Review Letters* **81**, 5932 (1998).
 - [2] W. Dür, H.-J. Briegel, J. Cirac, and P. Zoller, *Physical Review A* **59**, 169 (1999).
 - [3] M. Żukowski, A. Zeilinger, M. Horne, and A. Ekert, *Physical Review Letters* **71**, 4287 (1993).
 - [4] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. Wootters, *Physical Review Letters* **76**, 722 (1996).
 - [5] D. Deutsch, A. K. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *Physical Review Letters* **77**, 2818 (1996).
 - [6] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, *Nature* **414**, 413 (2001).
 - [7] P. van Loock, T. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, *Physical Review Letters* **96**, 240501 (2006).
 - [8] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, *Review of Modern Physics* **83**, 33 (2011).
 - [9] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, *Physical Review A* **87**, 052315 (2013).
 - [10] S. Bratzik, S. Abruzzo, H. Kampermann, and D. Bruß, *Physical Review A* **87**, 062335 (2013).
 - [11] L. Jiang, J. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, *Physical Review A* **79**, 032325 (2009).
 - [12] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, *Nature Photonics* **4**, 792 (2010).
 - [13] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, (2013), arXiv:1310.5291v1.
 - [14] A. Calderbank and P. Shor, *Physical Review A* **54**, 1098 (1996).
 - [15] A. Steane, *Proc. R. Soc. A* **452**, 2551 (1996).
 - [16] D. Gottesman and I. Chuang, *Nature* **402**, 390 (1999).
 - [17] X. Zhou, D. Leung, and I. Chuang, *Physical Review A* **62**, 052316 (2000).
 - [18] L. Jiang, J. Taylor, A. Sørensen, and M. D. Lukin, *Physical Review A* **76**, 062323 (2007).
 - [19] M. Nielsen and I. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).
 - [20] I. Devetak and A. Winter, *Proc. R. Soc. A* **461**, 207 (2005).
 - [21] D. Bruß, *Physical Review Letters* **81**, 3018 (1998).
 - [22] H. Bechmann-Pasquinucci and N. Gisin,

- Physical Review A **59**, 4238 (1999).
- [23] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Reviews of Modern Physics* **81**, 1301 (2009).
 - [24] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984) p. 175.
 - [25] N. K. Bernardes, L. Praxmeyer, and P. van Loock, *Physical Review A* **83**, 012323 (2011).
 - [26] S. Abruzzo, H. Kampermann, and D. Bruß, *Physical Review A* **89**, 012303 (2013).